Année Scolaire 2013-2014

Projet 1 : Mise en œuvre d'une nouvelle architecture réseau

Dossier Technique

Franck FALCHI
BTS SIO2 – PPE3

Table des matières

I- Contexte 2

II- Cahier des charges 3

III- Contraintes à respecter 3

IV- Besoin 4

4.1 Plan d'adressage 4

4.2 Schémas réseaux 5

4.3 Utilitaire 6

4.4 Configuration des routes 6

4.5 Configuration du filtrage sous WS2003 7

4.1- Mode d'emploi 7

4.2- Règles de filtrage 8

4.6 Installation d'IIS sur 1.129 & 0.119 11

4.7 Installation d'un contrôleur de domaine dans le réseau SR1 12

I- Contexte

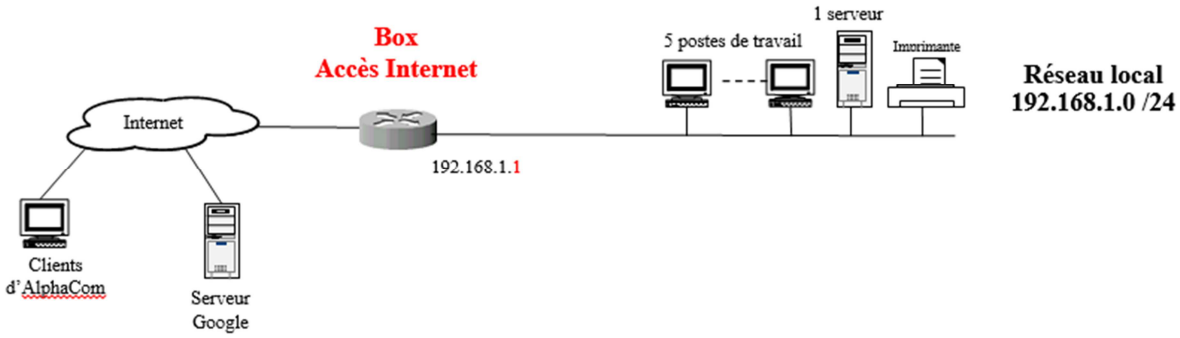
L'entreprise « AlphaCom » est une petite société dont l'activité est le secrétariat téléphonique. La majorité de ses clients travaillent dans le secteur médical (médecins, chirurgiens, spécialistes, etc.). Les services proposés par l'entreprise portent essentiellement sur la gestion des rendez-vous entre un client (médecin ….) et ses patients.

Les agendas des clients sont traités, en interne, sous Excel. Seules les secrétaires d'AlphaCom peuvent les modifier. En règle générale, les agendas sont transmis au client en fin de journée, soit par fax, soit par email ou soit par téléphone.

Avec le développement d'Internet, certains clients ont exprimé le besoin de pouvoir accéder à leur agenda (lecture et modification) depuis leur lieu de travail. L'entreprise AlphaCom a alors décidé d'utiliser le partage de documents proposé par Google.

Le principal inconvénient des documents Google est que leur format n'est pas entièrement compatible avec celui d'Excel. Cela oblige donc AlphaCom à gérer des documents simultanément sous les deux formats.

L'architecture du réseau actuel

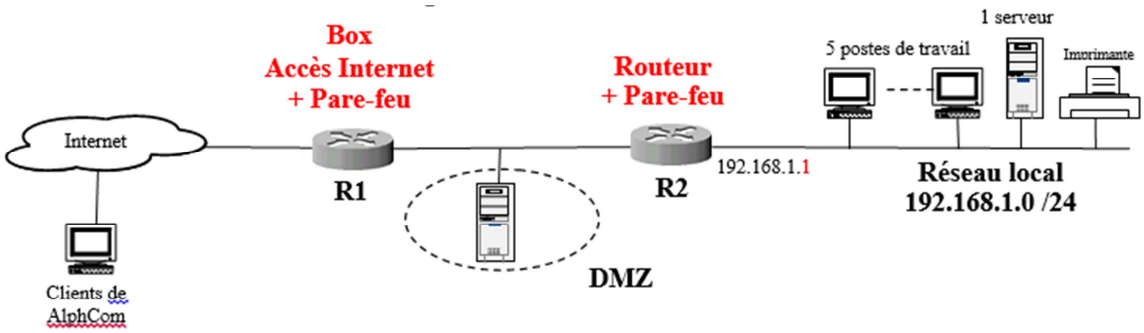


Les changements souhaités par « AlphaCom »

L'entreprise souhaite harmoniser ses documents de travail (agendas) en ne conservant que le format Microsoft Excel. Elle souhaite ne plus dépendre de Google et pouvoir gérer entièrement ses documents.

Pour cela, elle envisage de mettre en place une nouvelle machine qui sera située dans ses locaux et sur laquelle seront mis à disposition les documents devant être accessibles depuis Internet, par les clients qui en feront la demande.

La nouvelle architecture réseau envisagée



II- Cahier des charges

- Cc1 : La machine située dans la DMZ hébergera uniquement les documents Excel qui doivent être accessibles depuis Internet par les clients d'AlphaCom. Ces documents devront également être accessibles depuis le réseau local par les secrétaires.
- Cc2 : Les clients de l'entreprise (via Internet) ne devront pouvoir accéder qu'à la DMZ et surtout pas au réseau local.
- Cc3 : Les secrétaires d'AlphaCom (réseau local) devront pouvoir accéder à la DMZ (Mise à jour des agendas) et également à Internet.
- Cc4 : Tous les employés d'AlphaCom ne pourront accéder au réseau local qu'après identification (login et mot de passe, puis ouverture de session). A traiter dans la deuxième partie du PPE.
- Cc5 : Les fichiers situés sur la machine de la DMZ devront être sauvegardés tous les jours sur le serveur du réseau local. Il faudra s'assurer qu'en cas de destruction d'un document de la DMZ on puisse le restaurer.

III- Contraintes à respecter

- C1 : Utiliser des machines virtuelles.
- C2 : Les postes des clients Internet et les postes de travail du réseau local seront simulés par des machines Windows7 ou XP Pro.
- C3 : Les routeurs seront des machines Windows server 2003 (ou 2008, au choix).

- C4 : Pour les tests, il faudra prévoir une quantité de machines la plus petite possible.
- C5 : Vous n'utiliserez pas réellement Internet. Les postes représentant un client (Internet) de l'entreprise seront directement connectés au routeur simulant l'accès à Internet.
- C6 : Les cinq premières adresses de chaque plage seront réservées pour les serveurs (imprimantes). Les routeurs utiliseront les adresses IP les plus hautes dans la plage.
- C7 : Durée de réalisation : 2 séances de 4h.

IV- Besoin

4.1 Plan d'adressage

On aura besoin de deux SR pour l'entreprise. On utilisera un troisième SR qui correspondra à Internet dans notre cas « Numéricâble »

IP de l'entreprise : **192.168.1.0 /24**

Un bit pour les SR, 2^1 = **2** SR.

Il reste 8-1= 7 bits pour les identifient hôtes donc 2^7-2= **126** hôtes par SR.

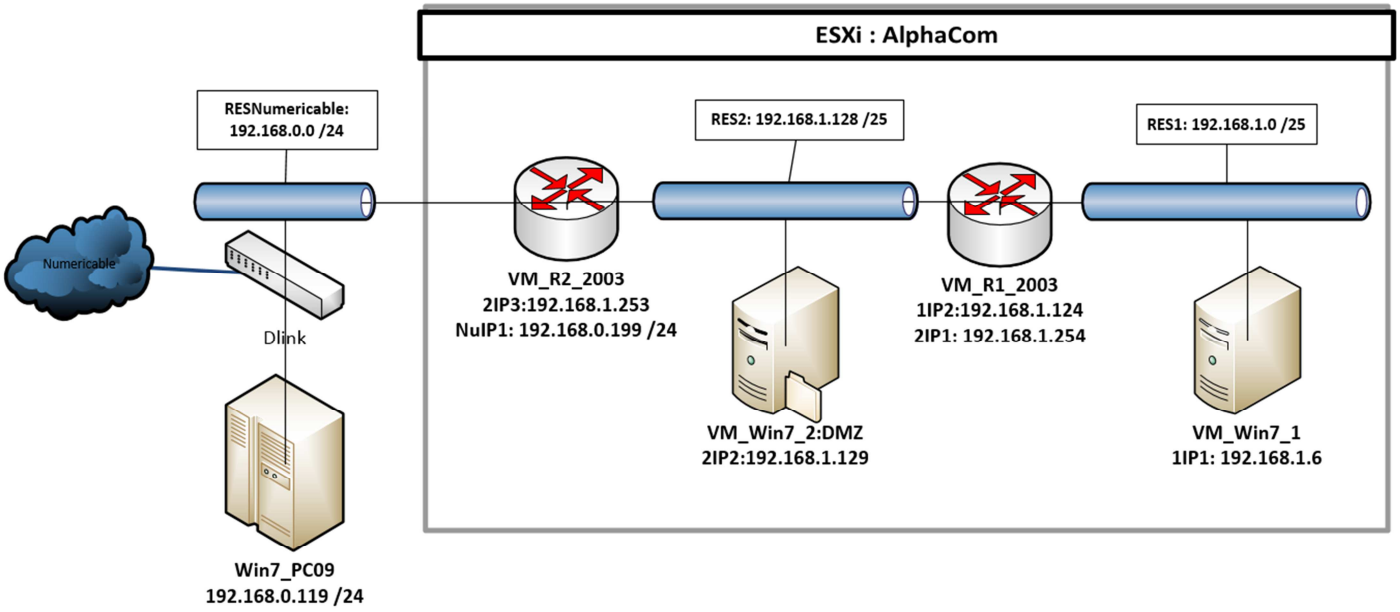
Le nouveau masque de l'entreprise est **/25** (255.255.255.128).

Je nommerai SR1 pour le réseau local, SR2 pour la DMZ et SRNum pour Internet.

SR	Nom	IP et Mas	Plage IP	Plage IP Sr/Imp	Plage IP PC	IP Routeur	Broadcaste
SR1	Local	192.168.1.0 /25	1.1 à 124	1.1 à 1.5	1.6 à 1.122	1.124	1.125
SR2	DMZ	192.168.1.128 /25	129 à 254	1.129 à 1.133	1.134 à 1.252	1.253 Et 1.254	1.255
SRNu	Inte	192.168.0.1	xx	xxxx	xxx	0.199	

IP		Passerelle	Masq
R1	Interface 1 = 1.124 Interface 2 = 1.254		/25
R2	Interface 1 = 1.253 Interface 2 = 0.199		/25
VM_Win7_1	192.168.1.6	192.168.1.124	/25
VM_Win7_2:DMZ	192.168.1.129	192.168.1.253	/25
Win7_PC09	192.168.0.119	192.168.0.199	/24

4.2 Schémas réseau



4.3 Utilitaire

- Deux routeurs virtuels sous Windows 2003 nommé « VM_R1_2003 » et « VM_R2_2003 »
- Deux clients virtuels sous Windows 7, dont un pour la DMZ nommé « VM_Win7_2:DMZ » et l'autre nommé « VM_Win7_1 » pour la secrétaire
- Le poste physique client « SIOPC09 », office d'internet pour les clients de l'entreprise
- Création de deux cartes réseaux virtuel pour chaque routeur
- Création de deux commutateurs virtuels nommés respectivement Res1 et Res2 pour brancher les cartes réseaux des routeurs et des clients
- Désactivation sur tous les postes du pare feu
- Je débrancherai la connexion Internet du routeur Numéricâble pour ne pas avoir des conflits d'adresse
- Logiciel Wireshark pour regarder les trames et Mozilla pour faire des tests Web
- Installation du service IIS sur la DMZ et sur le client Win7_PC09 pour test

Pour le poste « VM_Win7_2:DMZ » j'activerai un dossier de partage pour le fichier Excel. Et je configurerai sur ce poste une sauvegarde automatique proposé par Windows tous les jours à 20h concernant le fichier Excel sur un dossier de partage du poste « VM_Win7_1 » accessible par un mot de passe.

4.4 Configuration des routes

J'utiliserai le routage dynamique pour faciliter la connexion entre les routeurs.

Pour cela, allez dans ***Routage et accès distant*** puis ***Routage IP / Général***. Faites un clic droit et choisissez l'option ***Ajouter un protocole de routage***. Sélectionnez le protocole ***RIP***.

Le nouveau protocole étant installé sur le routeur, il faut ensuite lui préciser les interfaces du routeur sur lesquelles il va être actif. Faites un clic droit sur RIP puis ***Nouvelles interfaces*** et rajouter les 2 interfaces de votre routeur.

Allez également dans les propriétés du protocole RIP et modifiez le « délai d'attente du routeur avant qu'il n'envoie des mises à jour déclenchées ». Passez la valeur de 5 à 10 secondes.

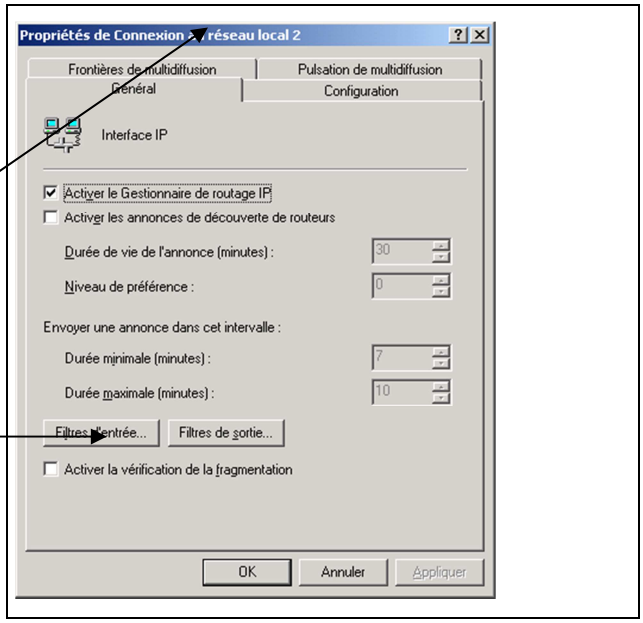
4.5 Configuration du filtrage sous WS2003

4.1- Mode d'emploi

J'appliquerai des règles de filtrage pour sécuriser la DMZ et le réseau local.

Le service qui permet de gérer le filtrage est le service « ***Routage et accès distant*** » Pour accéder à la fonction de filtrage, il faut sélectionner « ***Routage IP, puis Général*** ». On peut ainsi visualiser et accéder aux interfaces du routeur.

Ensuite, il faut sélectionner l'interface sur laquelle on veut mettre en œuvre le filtrage.
Pour cela, faire un clic droit puis sélectionner « Propriétés » de l'interface en question (dans l'exemple « Connexion au réseau local 2) :



Choisir ensuite le type de filtrage : « Filtre d'entrée » ou « Filtre de sortie »

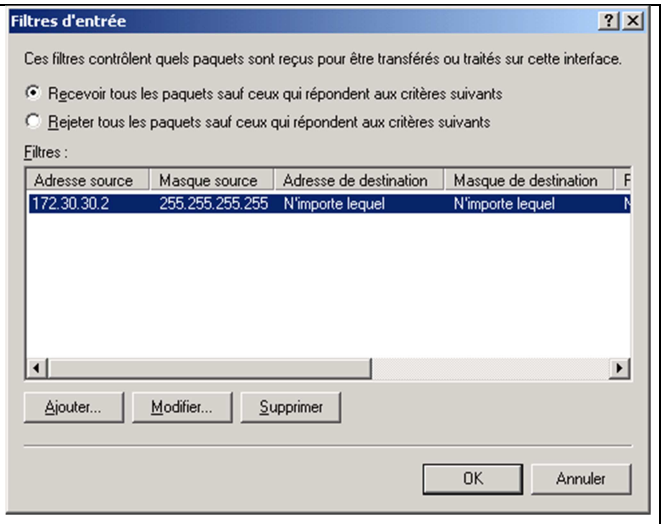
Le filtre offre deux options :

1. ***Recevoir*** tous les paquets sauf ceux qui répondent aux critères de la règle.
2. ***Rejeter*** tous les paquets sauf ceux qui répondent aux critères de la règle.

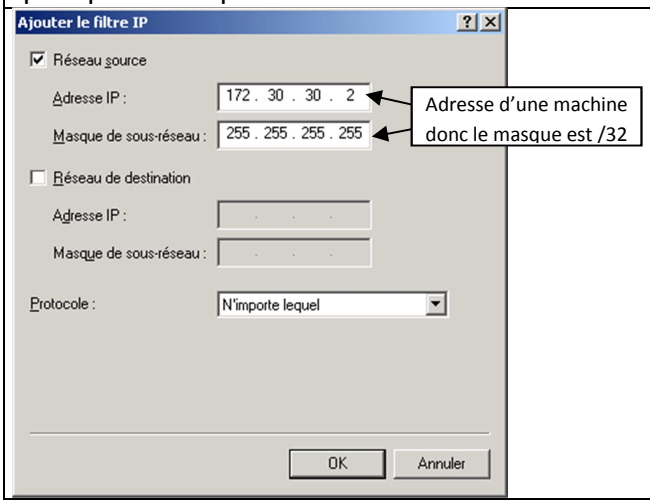
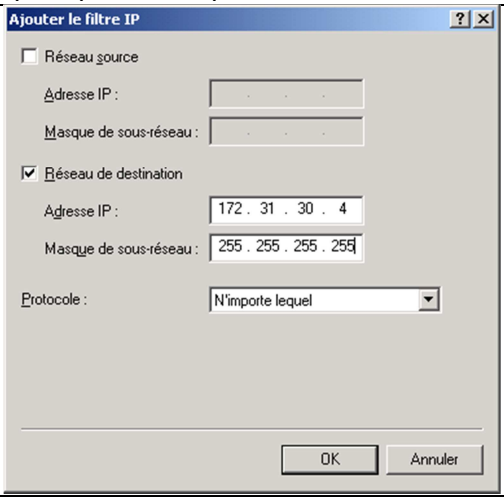
Une règle de filtrage peut agir en fonction des critères suivants :

- Adresse source et Masque source,
- Adresse destination et Masque destination,
- Protocole ;
- Port source et Port destination

Les fonctions des boutons « Ajouter », « Modifier » ou « Supprimer » sont classiques à Windows.

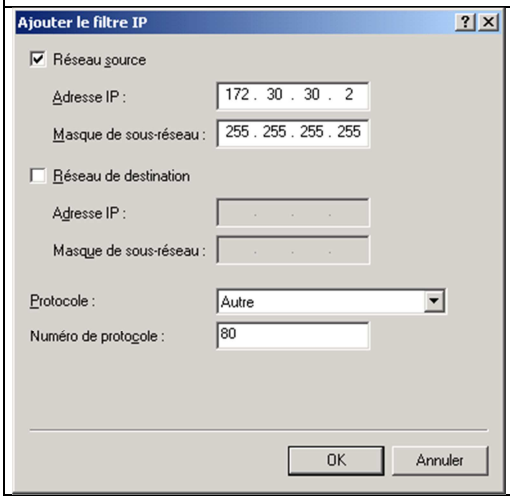
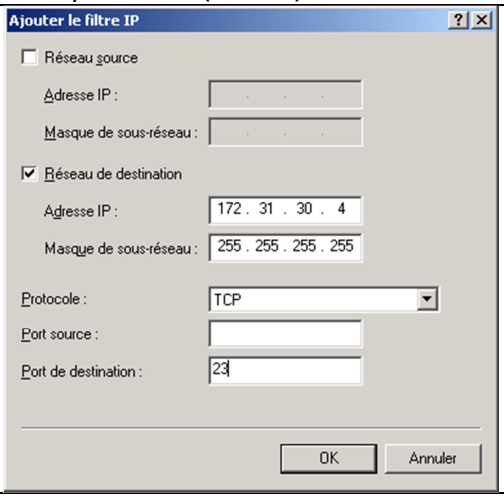


Lors de l'ajout d'une règle, plusieurs possibilités sont offertes telles que:

Filtrage sur un poste du réseau source, quel que soit le protocole utilisé :	Filtrage sur un poste du réseau destination, quel que soit le protocole utilisé :
	

Ajouter le filtre IP
Réseau source
Adresse IP : 172 . 30 . 30 . 2
Masque de sous-réseau : 255 . 255 . 255 . 255
Adresse d'une machine donc le masque est /32
Réseau de destination
Adresse IP :
Masque de sous-réseau :
Protocole : N'importe lequel
OK
Annuler

Ajouter le filtre IP
Réseau source
Adresse IP :
Masque de sous-réseau :
Réseau de destination
Adresse IP : 172 . 31 . 30 . 4
Masque de sous-réseau : 255 . 255 . 255 . 255
Protocole : N'importe lequel
OK
Annuler

Filtrage sur la source et sur le protocole utilisé comme par exemple http dont le n° est 80	Filtrage sur la destination et sur le port de destination Ici le port n°23 (Telnet) :
	

Ajouter le filtre IP
Réseau source
Adresse IP : 172 . 30 . 30 . 2
Masque de sous-réseau : 255 . 255 . 255 . 255
Réseau de destination
Adresse IP :
Masque de sous-réseau :
Protocole : Autre
Numéro de protocole : 80
OK
Annuler

Ajouter le filtre IP
Réseau source
Adresse IP :
Masque de sous-réseau :
Réseau de destination
Adresse IP : 172 . 31 . 30 . 4
Masque de sous-réseau : 255 . 255 . 255 . 255
Protocole : TCP
Port source :
Port de destination : 23
OK
Annuler

Vous remarquerez dans le dernier exemple, Filtrage sur la destination et sur le port de destination n°23 (Telnet), qu'il faut préciser le protocole de transport utilisé, TCP (ou éventuellement UDP).

4.2- Règles de filtrage

Protection du réseau local : cc1 et cc2

l'interface concernée : en entrée 192.168.0.199

Quelle action de filtrage faut-il choisir ? [ ] Recevoir tous [x] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Port Sce	Port Dest
				HTTP	80	80

l'interface concernée : en entrée 192.168.0.199

Quelle action de filtrage faut-il choisir ? [ ] Recevoir tous [x] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Port Sce	Port Dest
				TCP établie	80	80

Permet d'accéder au serveur DMZ et de bloquer les Pings sur cette interface, ainsi cela permet au réseau 1 d'accéder à internet et de recevoir la requête réponse.

Règles pour interdire les pings sur les interfaces des routeurs

l'interface concernée : en entrée 192.168.1.253

Quelle action de filtrage faut-il choisir ? [x] Recevoir tous [ ] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Type	Code

N'importe lequel	N'importe lequel	192.168.1.253	255.255.255.255	ICMP	8	0

l'interface concernée : en entrée 192.168.1.254

Quelle action de filtrage faut-il choisir ? [x] Recevoir tous [ ] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Type	Code
N'importe lequel	N'importe lequel	192.168.1.254	255.255.255.255	ICMP	8	0

l'interface concernée : en entrée 192.168.1.124

Quelle action de filtrage faut-il choisir ? [x] Recevoir tous [ ] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Type	Code
N'importe lequel	N'importe lequel	192.168.1.124	255.255.255.255	ICMP	8	0

l'interface concernée : en entrée 192.168.0.199

Quelle action de filtrage faut-il choisir ? [ ] Recevoir tous [x] Rejeter tout

Adr Sce	Masque Sce	Adr Dest	Masque Dest.	Protocole	Type	Code

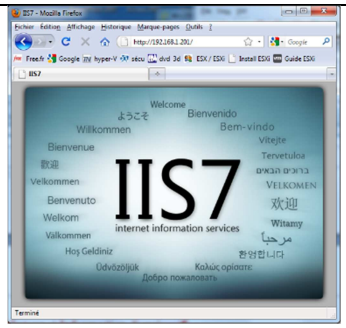
Pas besoin de règle de filtrage pour bloquer les pings sur cette interface car on rejette tout

4.6 Installation d'IIS sur 1.129 & 0.119

Aller dans « ajouter désactivé des fonctionnalités Windows » et sélection IIS si vous utilisez Windows7.

Pour un serveur :

Pour installer IIS, il faut tout d'abord ajouter le rôle « **Serveur web (IIS)** ».
Validez les *services de rôle* proposés par défaut et lancez l'installation.
Ouvrez la console ***Gestionnaire des services internet (IIS).***
Dans la partie de gauche, sélectionnez votre machine (serveurXX).
Vous devez ensuite voir 2 sous menus : ***Pools d'applications*** et ***Sites***.
Si vous sélectionnez Sites vous devriez voir ***Default Web Site*** qui est le site web par défaut proposé par IIS.

Pour vérifier le bon fonctionnement du site web, ouvrez le navigateur sur votre poste client et tapez l'URL « **http:// IP de votre serveur »**. Votre navigateur doit alors afficher la page d'accueil du site (ci-contre). Comme tout le monde a la même page, vous allez la modifier et la personnaliser. Ainsi, lorsque vous ferez des tests, vous serez sûr que vous accèderez à votre serveur et non à celui du voisin. Le document HTML qui contient la page d'accueil se trouve sous : ***C:\inetpub\wwwroot*** et se nomme « ***iisstart.html*** ».	

Ouvrez le document ***iisstart.html*** avec le bloc note.
Vers la fin du fichier recherchez la ligne suivante :

```
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="411" /></a>
```

Mettez cette ligne en commentaire et rajouter le texte "SERVEURxx" comme suit:

```
< !--
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="411" /></a>
-->
SERVEUR01 (le 01 étant à remplacer par le numéro de votre serveur)
```

Faire le test sur le poste 1.6 pointant vers 0.119 pour vérifier la connexion internet.
Faire le test sur le poste 0.119 pointant vers 1.129 pour vérifier la connexion au serveur DMZ.

4.7 Installation d'un contrôleur de domaine dans le réseau SR1

J'utiliserai une VM avec Serveur 2008 R2 avec la configuration suivante :

Nom du domaine : Domaine09.BTS.local

IP fixe : 192.168.1.1

Masque : 255.255.255.128

Passerelle : 192.168.1.124

DNS : 192.168..119

Création des utilisateurs

Pour créer des utilisateurs, vous avez deux façons de faire. Soit vous passez par le menu, onglet ***ACTION*** puis ***NOUVEAU*** et enfin ***UTILISATEUR***. Soit vous faites un clic droit dans la partie droite (celle où apparaissent des utilisateurs déjà existants) puis dans le menu contextuel sélectionner ***NOUVEAU*** et enfin ***UTILISATEUR.*** L'assistant de création d'utilisateur se lance.

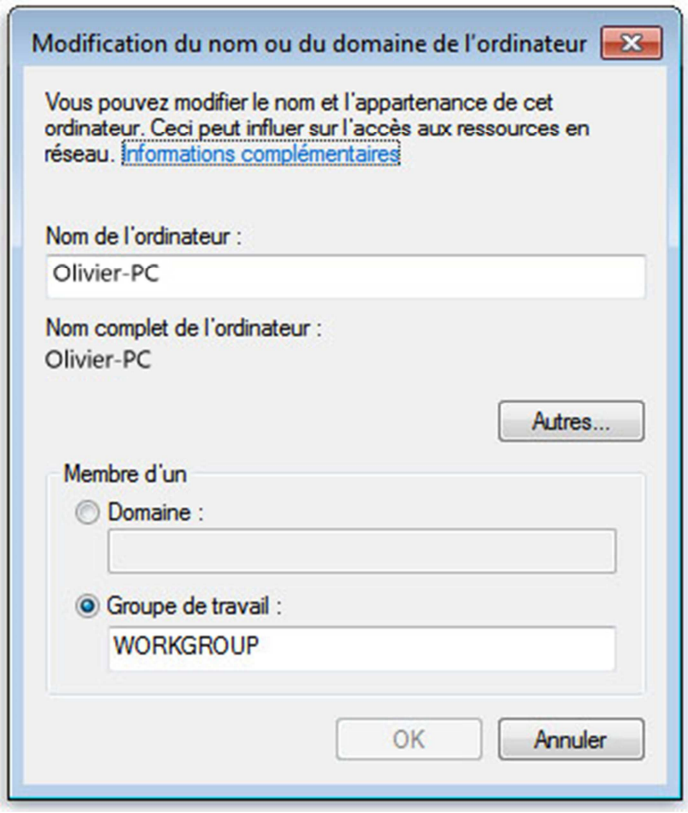
Le poste client aura la même configuration que la VM_Win7_1. Il faudra le mettre sur le domaine.

1. Pour ouvrir Système, cliquez sur le bouton **Démarrer** , faites un clic droit sur **Ordinateur**, puis cliquez sur **Propriétés**.

2. Sous **Paramètres de nom d'ordinateur, de domaine et de groupe de travail**, cliquez sur **Modifier les paramètres**. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.

3. Sous l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier**. Vous pouvez également cliquer sur **ID réseau** pour utiliser l'Assistant Joindre un domaine ou un groupe de travail afin d'automatiser le processus de connexion à un domaine et de création d'un compte d'utilisateur de domaine sur votre ordinateur.

4. Sous **Membre d'un**, cliquez sur **Domaine**.


Modification du nom ou du domaine de l'ordinateur
Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ceci peut influer sur l'accès aux ressources en réseau. Infomations complémentaires
Nom de l'ordinateur :
Olivier-PC
Nom complet de l'ordinateur :
Olivier-PC
Autres...
Membre d'un
Domaine :
Groupe de travail :
WORKGROUP
OK
Annuler
Boîte de dialogue Modification du nom ou du domaine de l'ordinateur

5. Tapez le nom du domaine que vous souhaitez rejoindre, puis cliquez sur **OK**.

   Vous serez invité à taper vos noms d'utilisateurs et mot de passe pour le domaine.

   Une fois que vous avez rejoint le domaine, vous êtes invité à redémarrer votre ordinateur. Vous devez redémarrer votre ordinateur pour que les modifications prennent effet.